Discounted Duration Calculus

Work in Progress

H. Ody

Joint work with M. Fränzle and M. R. Hansen

October 19, 2015

SCARE
System Correctness
under Adverse Conditions

CARL VON OSSIETZKY universität OLDENBURG

‘Eventually properties’ are common

Booting Eventually the system is ready

'Eventually properties' are common

Booting	Eventually the system is ready
Access to shared Resource	After a request, Eventually we get a grant

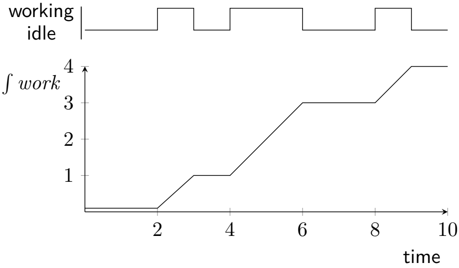
'Eventually properties' are common

Booting	Eventually the system is ready
Access to shared Resource	After a request, Eventually we get a grant

- Often Soon is better than Eventually
- Want quantitative statements about eventually properties
- Truth value is in interval $[0, 1]$

Motivation

Discounting in Duration Caluclus

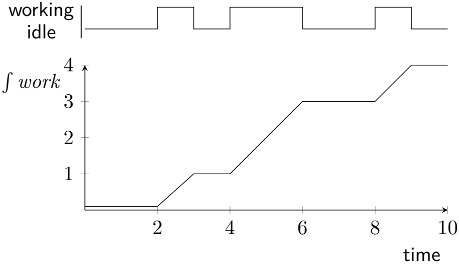


Example - Energy Consumption

- Working consumes energy
- Idle conserves energy
- Property: The energy lasts long

Motivation

Discounting in Duration Caluclus

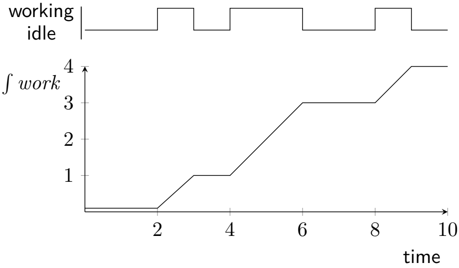


Example - Energy Consumption

- Working consumes energy
- Idle conserves energy
- Property: The energy lasts long

Example - Job Completion

- Job needs a fixed duration of work to finish
- Property: The job is finished soon



Example - Energy Consumption

- Working consumes energy
- Idle conserves energy
- Property: The energy lasts long

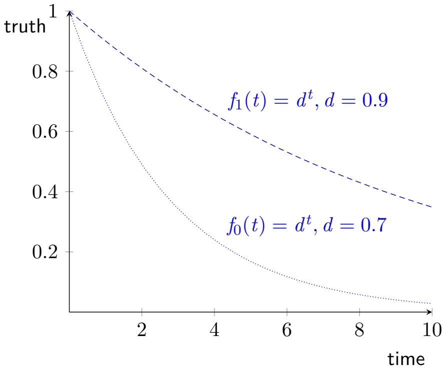
Example - Job Completion

- Job needs a fixed duration of work to finish
- Property: The job is finished soon

We want properties over durations

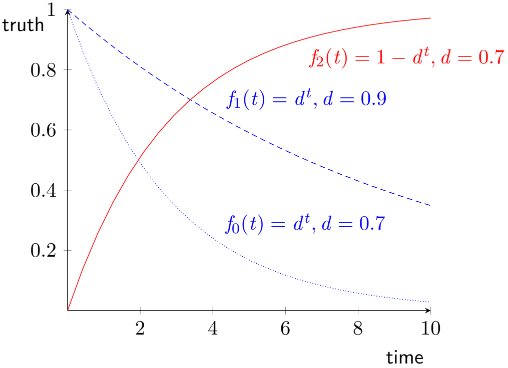
Truth value ...

- ... is a real number from interval $[0, 1]$
- ... represents quality of a system or our satisfaction with the system
- $\mathrm{F}^{d}\phi$ The earlier a good state is reached the better



Truth value ...

- ... is a real number from interval $[0, 1]$
- ... represents quality of a system or our satisfaction with the system
- $\mathrm{F}^d\phi$ The earlier a good state is reached the better
- $\mathrm{G}^d\phi$ The later a bad state is reached the better



Discounting - Background

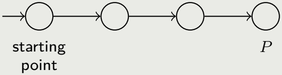
- Introduction in economics [Sam37]
- Introduced into temporal logics in [DAFH$^+$04] (Discounted CTL)
- Definition of discounted LTL [ABK14]

Background and Intuition

Discounting in LTL and CTL

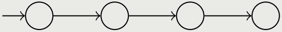
Example

- $\mathrm{F}^{0.7}P$ on path π :



- Discount is the basis
- Time of satisfaction is the exponent

Example

- $\mathrm{F}^{0.7} P$ on path π : 

- Discount is the basis
- Time of satisfaction is the exponent

Truth value is

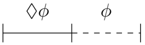
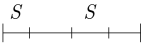
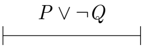
$$\begin{aligned} \mathcal{I}[\![\mathrm{F}^{d} P, \pi]\!] &= \sup_{0 \leq t}\{0.7^{t} \cdot \mathcal{I}[\![P, \pi[t..]]\!]\} \\ &= 0.7^{3} \cdot \mathcal{I}[\![P, \pi[3..]]\!] \\ &= 0.343 \cdot \mathcal{I}[\![P, \pi[3..]]\!] \end{aligned}$$

Discounted Duration Calculus

Syntax

$$\phi ::= \Diamond^d \phi \mid \int^d S \geq c \mid \int^d S > c \mid \neg \phi \mid \phi \vee \phi$$
$$S ::= P \mid \neg S \mid S \wedge S \quad .$$

P is a Boolean proposition

$\Diamond \phi$	There is a neighbouring interval satisfying ϕ	
$\int S \geq c$	State expression S holds for at least c	
	Following abbreviations can be expressed	
$\lceil P \vee \neg Q \rceil$	State expression $P \vee \neg Q$ holds in this interval	
$\Box \phi$	ϕ is satisfied on all neighbouring intervals	

Discounted Duration Calculus

Semantics

$$\mathcal{I}[\![\Diamond^d \phi]\!](tr, [k, m]) = \sup_{l \geq m} \{ d^{l-m} \cdot \mathcal{I}[\![\phi]\!](tr, [m, l]) \}$$

$$\mathcal{I}[\![\textstyle\int S \geq c]\!](tr, [k, m]) = \begin{cases} 0 & \text{if } \int_{t=k}^{m} S(t)\,\mathrm{d}t < c \\ 1 & \text{otherwise} \end{cases}$$

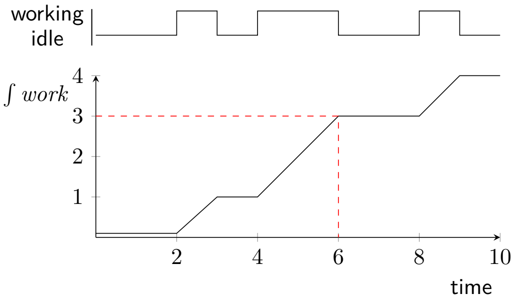
$$\mathcal{I}[\![\neg\phi]\!](tr, [k, m]) = 1 - \mathcal{I}[\![\phi]\!](tr, [k, m])$$

$$\mathcal{I}[\![\phi_0 \vee \phi_1]\!](tr, [k, m]) = \max\{\mathcal{I}[\![\phi_0]\!](tr, [k, m]), \mathcal{I}[\![\phi_1]\!](tr, [k, m])\}$$

Example

Statements over durations

- $\Box^d \int work < 3$

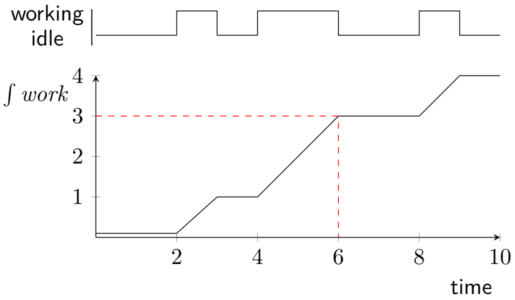


$$\mathcal{I}[\![\Box^d \int work < 3]\!](tr, [k, m])$$
$$= \mathcal{I}[\![\neg\Diamond^d \neg \int work < 3]\!](tr, [k, m])$$

Example

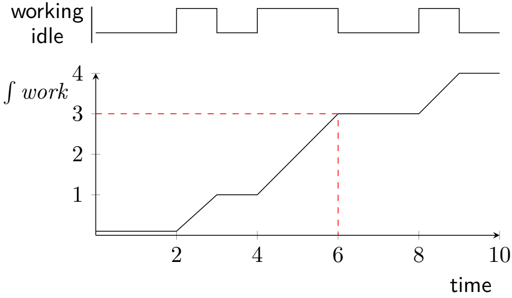
Statements over durations

- $\Box^d \int work < 3$



$$\mathcal{I}[\![\Box^d \int work < 3]\!](tr, [k, m])$$
$$= \mathcal{I}[\![\neg \Diamond^d \neg \int work < 3]\!](tr, [k, m])$$
$$= 1 - \sup_{l \geq m}\{d^{l-m} \cdot \mathcal{I}[\![\neg \int work < 3]\!](tr, [m, l])\}$$

Example



Statements over durations

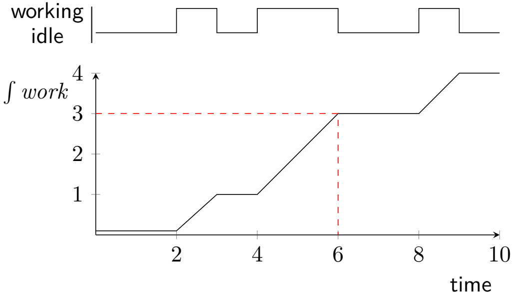
- $\Box^d \int work < 3$

$$
\begin{aligned}
&\mathcal{I}[\![\Box^d \textstyle\int work < 3]\!](tr, [k, m]) \\
&= \mathcal{I}[\![\neg\Diamond^d \neg \textstyle\int work < 3]\!](tr, [k, m]) \\
&= 1 - \sup_{l \geq m}\{d^{l-m} \cdot \mathcal{I}[\![\neg \textstyle\int work < 3]\!](tr, [m, l])\} \\
&= 1 - \sup_{l \geq m}\{d^{l-m} \cdot (1 - \mathcal{I}[\![\textstyle\int work < 3]\!](tr, [m, l]))\}
\end{aligned}
$$

Example

Statements over durations

- $\Box^d \int work < 3$



$$\begin{aligned}
&\mathcal{I}[\![\Box^d \int work < 3]\!](tr,[k,m]) \\
&= \mathcal{I}[\![\neg\Diamond^d \neg \int work < 3]\!](tr,[k,m]) \\
&= 1 - \sup_{l \geq m}\{d^{l-m} \cdot \mathcal{I}[\![\neg \int work < 3]\!](tr,[m,l])\} \\
&= 1 - \sup_{l \geq m}\{d^{l-m} \cdot (1 - \mathcal{I}[\![\int work < 3]\!](tr,[m,l]))\}
\end{aligned}$$

with $d = 0.7, m = 0$ $\quad = 1 - 0.7^6 = 0.88$

Questions of Decidability

The formulas we consider

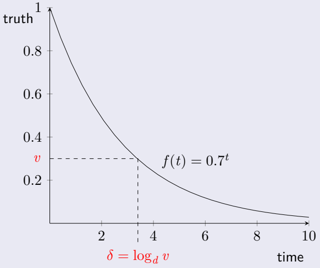
- In negation normal form
- No nested modalities and
- All modalities are discounted

Threshold Satisfiability

Sketch

We can decide $\exists tr.\,\mathcal{I}[\![\phi, tr]\!] \sim v$ with $\sim \in \{<, >, \geq, \leq\}$

- Example $\exists tr.\,\mathcal{I}[\![\phi, tr]\!] \geq v$ with $\phi \equiv \Diamond^{0.7} \int work \geq c$



Truthvalue of $\Diamond^{d}\phi$ when ϕ is satisfied at time t

Questions of Decidability

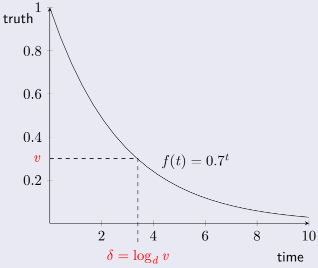
The formulas we consider

- In negation normal form
- No nested modalities and
- All modalities are discounted

Threshold Satisfiability — Sketch

We can decide $\exists tr.\,\mathcal{I}[\![\phi, tr]\!] \sim v$ with $\sim \in \{<, >, \geq, \leq\}$

- Example $\exists tr.\,\mathcal{I}[\![\phi, tr]\!] \geq v$ with $\phi \equiv \Diamond^{0.7} \int work \geq c$
- Transform ϕ into a time-bounded linear hybrid automaton A_ϕ (reachability is decidable) [BDG+11]
- A_ϕ has a location reachable iff $\int work \geq c$ is satisfied in at most δ time



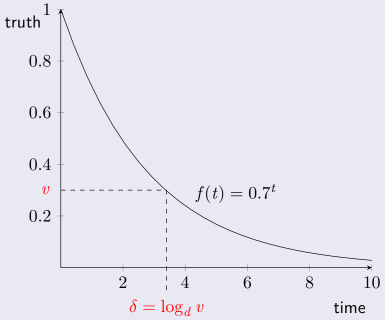
Truthvalue of $\Diamond^d \phi$ when ϕ is satisfied at time t

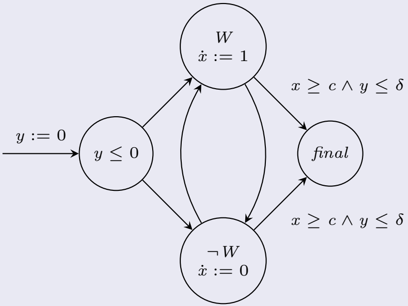
Example

$\exists tr.\, \mathcal{I}[\![\Diamond^{0.7} \int work \geq c, tr]\!] \geq v$

Threshold Satisfiability

Sketch





Questions of Decidability

Model Checking — Sketch

Let M be a timed automaton with only clock constraints of the form $x \sim c$, i.e. no comparisons of clocks

- Model checking is $\forall tr \in M . \mathcal{I}[\![\phi, tr]\!] \geq v$
- Equivalently: $\neg \exists tr \in M . \mathcal{I}[\![\phi, tr]\!] < v$
- Check $\exists tr \in M . \mathcal{I}[\![\phi, tr]\!] < v$ on $M \otimes A_\phi$
- A witnessing trace constitutes a counter example

Conclusion

- Gave several examples to show usefulness of our logic
- Some meaningful questions are decidable
- Nested modalities pose a challenge
  I believe I have a procedure for approximate threshold satisfiability

Nested Modalities

Service should be online soon, and then run for a long time $\Diamond^{d_0}\Box^{d_1}\lceil S\rceil$

Future

- Formal proofs of decidability
- Implementation and case studies?

Shaull Almagor, Udi Boker, and Orna Kupferman.
Discounting in LTL.
In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 424–439. Springer, 2014.

Thomas Brihaye, Laurent Doyen, Gilles Geeraerts, Joël Ouaknine, Jean-Fraņcois Raskin, and James Worrell.
On reachability for hybrid automata over bounded time.
In *Automata, Languages and Programming*, pages 416–427. Springer, 2011.

Luca De Alfaro, Marco Faella, Thomas A Henzinger, Rupak Majumdar, and Mariëlle Stoelinga.
Model checking discounted temporal properties.
Springer, 2004.

Paul A Samuelson.
A note on measurement of utility.
The Review of Economic Studies, 4(2):155–161, 1937.

I think we are able to decide approximate threshold satisfiability, i.e. $\exists tr \in M . \mathcal{I}[\![\phi, tr]\!] \sim v \pm \epsilon$

Example

Consider $\Diamond^{d_0} \Box^{d_1} \psi$

- We evaluate the formula at some timepoint δ_i
- The satisfaction value is $d^{\delta_i} \cdot \mathcal{I}[\![\Box^{d_1} \psi, tr]\!]$
- Then the comparison is satisfied iff

$$\mathcal{I}[\![\Box^{d_1} \psi, tr[\delta_i..]]\!] \geq \frac{v}{d^{\delta_i}}$$

- If we pick enough points δ_i at which to try satisfying $\Box^{d_1} \psi$ then we should come within ϵ distance of v, if that is possible at all
- As the discounting formula is exponential hopefully we do not need too many δ_i..?